UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,019	01/08/2002	Zheng Qi	BRCMP007/BP-1687	4910

7590 09/15/2005

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
ALOMARI, FIRAS B	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/042,019	QI, ZHENG	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/28/02,1/21/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 5-7, 10 and 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook et al. US (6,334,190) in view of Sait et al..

Regarding claim 1 & 10: Silverbrook discloses an authentication engine architecture for a SHA-1 multi-round authentication algorithm, comprising: a hash engine configured to implement hash round logic for an SHA1 authentication algorithm (*Col 11, lines 9-27*), but he doesn't disclose the hash round logic implementation including, a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA). However Sait teaches a plurality of adder trees with a timing critical path having a single carry-ahead adder to perform multiplication in cryptographic operations (*Sait Figures 3 & 6, page 110 Col 2 Paragraphs 2 & 3*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine Silverbrook's system sait's technique to include a combined adder having a

single CLA. One would be motivated to so in order to enable the system to process large amount of data at high speeds (*Sait Page 109 Introduction*)

Regarding claims 5 & 16:Silverbrook and Sait in combination teach the authentication engine architecture of claim 1, wherein the combined adder tree is configured such that addition computations are conducted in parallel with round operations (*Figures 3 and 6, Page 110 Col 2, Paragraphs 2 and 3*).

Regarding claim 6: Silverbrook teaches the authentication engine architecture of claim 1, wherein the architecture is implemented as an authentication engine architecture for a multi-loop, SHA-1 authentication algorithm (Col 11, lines 4-9), comprising:

a first instantiation of an SHA-1 authentication algorithm hash round logic in an inner hash engine (*Col 7, lines 3-5 & Col 11, lines 9-27*);

a second instantiation of an SHA-1 authentication algorithm hash round logic in an outer hash engine (*Col 7, lines 3-5 & Col 11, lines 9-27)*;

a dual-frame payload data input buffer configured for loading one new data block while another data block one is being processed in the inner hash engine (Col 7, lines 3-5 & Col 45, lines 2-6);

an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations (Col 45, lines2-6); and

a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines (Col 38, lines 8-13).

Regarding claims 7 & 18:Silverbrook teaches the authentication engine architecture of claim 6, wherein the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (Col 11, lines 4-9).

Regarding claim 17: Silver brook teaches the method of claim 10, wherein said authentication engine is a multi-loop, multi-round authentication engine architecture having a hash engine core comprising an inner hash engine and an outer hash engine (Col 45, lines 2-6), said architecture configured to, pipeline hash operations of said inner hash and outer hash engines (Col 7, lines 3-5), collapse and rearrange multi-round logic to reduce rounds of hash operations, and implement multi-round logic such that addition computations are conducted in parallel with round operations (Col 11, lines 4-27).

Regarding claim 19: Silverbrook teaches the method of claim 18, wherein said pipelining comprises performance of an outer hash operation for one data payload in parallel with an inner hash operation of a second data payload in a packet stream fed to the authentication engine (Col 11, lines 9-27).

Regarding claim 20: The method of claim 19, wherein a dual-frame input buffer is used for the inner hash engine (Col 11, lines 9-27 & Col 45, lines 2-8).

Regarding claim 21: The method of claim 20, wherein initial hash states for the hash operations are double buffered for concurrent inner hash and outer hash operations (Col 45, lines 2-6).

Regarding claim 22: The method of claim 21, wherein concurrent constant lookups are performed from a dual-ported ROM by both inner and outer hash engines (Col 38, lines 6-15) .

3. Claims 2, 8-9, 11 and 13-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook et al. US (6,334,190) in view of Sait et al. as applied to claim 1 above, and further in view of Schneier "Applied Cryptography, Second Edition", John Wiley & Sons, New York, 1996, Pages 336-445.

Regarding claims 2 & 11: The system as combined in claim 1 teaches the authentication engine architecture of claim 1, but doesn't teach hash round logic implementation has a timing critical path equivalent to one of: one 5-bit addition, one 32-bit CSA, a multiplexer operation, and one 32-bit CLA; and three 32-bit CSAs, a multiplexer operation, and one 32-bit CLA. However Schneier taches one 5-bit addition, one 32-bit CSA, a multiplexer operation, and one 32-bit CLA; and three 32-bit CSAs, a multiplexer operation, and one 32-bit CLA (Pages 442-245) Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system as disclosed in claim 1 with

Schneier's teaching of the secure hash algorithm in order to help ensure the security of a message sent (Page 442).

Regarding claims 9 & 13: Silverbrook as combined in claim 1 doesn't teach the hash engine is configured to implement hash round logic comprising:
five hash state registers; one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative. However Schneier teaches a method for performing secure hashing algorithm (*Page 436 & Page 442*) where he teaches using five hash state registers (*Page 442, Description of SHA*) and one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative (*Page 442-445*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine Schneier teaching of secure hash algorithm with Silverbrook system. One would be motivated to do so in order to ensure the security of the messages being sent and exchanged in the system (*Page 442*).

Regarding claim 14: Schneier discloses the method of claim 13, wherein, in successive SHA1 rounds, registers having the critical path are alternative (Page 443-444 & Figure 18.7).

Regarding claims 8 & 15: Schneier discloses the method above, wherein eighty rounds of an SHA1 loop are collapsed into forty rounds (*Page 443, 2nd Paragraph*

& Page 444, Security of SHA 2nd Paragraph).

4. Claims 3-4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook et al. US (6,334,190) in view of Sait et al. as applied to claim 1 above, and further in view of Yokota et al. US (6,304,657).

Regarding claims 3 & 12: The system as combined above discloses the authentication engine architecture of claim 1 but doesn't teach the additions performed by the combined adder tree are preceded by a 5-bit circular shifter. However Yokota discloses an apparatus for performing cryptographic operations (Col 3, lines 42-56) where he teaches in the encoding operation of the plain text the adder is preceded by a (3, **5** or 7)-bit circular shift (*Col 15, lines 46-54; Col 15, line 63 through Col 16, line 3 & Col 16, lines 43-53*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to perform a 5-bit circular shifter operation after the adder operation. One ordinary skilled in the art would be motivated to do so in order to produce a significant randomness in the results which strengthen cryptographic security by producing a strong data shuffling and sufficient bit avalanche effect without decreasing the cryptographic speed of the system when using conventional techniques (*Col 3, lines 41-45 & Col 5, lines 10-15*)

Regarding 4:The authentication engine architecture as disclosed in claim 3

above, discloses the combined adder tree includes add5to1 and add4to1 adders (*Col 17, lines 15-35 & Col 18, lines 47-57*).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU 2131
9/9/05

Firas Alomari
Examiner
Art Unit 2136

FA